This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) A method of providing communications security, the method comprising:

(a) generating a protected content stream from a data stream;

(b) transmitting the protected content stream across a first short-range radio communications link; and

(c) transmitting across second short-range radio communications link information for converting the protected content stream into the data stream;

wherein the protected content stream comprises a packet, and wherein step (a) comprises inserting one or more errors into the packet.

2. (Canceled)

3. (Previously Presented) The method of claim 1, wherein step (a) further comprises inserting the one or more errors into a portion of the packet, the portion at a predetermined position within the packet.

4. (Original) The method of claim 3, wherein step (a) further comprises selecting the predetermined position.

5. (Original) The method of claim 3, wherein step (a) further comprises generating the one or more errors with a code.

6. (Original) The method of claim 5, wherein the code is based on a polynomial.

7. (Previously Presented) The method of claim 5, wherein step (c) comprises transmitting the predetermined position and the code across the second short-range radio communications link.

8. (Previously Presented) The method of claim 1, wherein the packet includes a field containing an error detection code and/or an error correction code, the method further comprising:

setting the error detection code and/or the error correction code after said inserting step.

9. (Original) The method of claim 8, wherein the error detection code and/or the error correction code includes a cyclical redundancy check (CRC) code.

10. (Original) The method of claim 1, wherein step (a) comprises:

formatting the data stream into a plurality of data packets, each the data packets including a field having an error detection code and/or error correction code;

generating at least one additional packet, the additional packet including a field having an error detection code and/or error correction code; and

arranging the at least one additional packet and the plurality of data packets into the protected content stream.

11. (Original) The method of claim 10, wherein the error detection codes and/or the error correction codes for the data packets and the at least one additional packet each include cyclical redundancy check (CRC) codes.

12. (Original) The method of claim 10, wherein step (a) further comprises randomly selecting a position of the at least one additional packet in the protected content stream.

13. (Previously Presented) The method of claim 10, wherein step (c) comprises transmitting across the second short-range radio communications link a position of the at least one additional packet in the protected content stream.

14. (Original) The method of claim 1, wherein step (a) comprises:

placing the data stream into a plurality of packets, each the packets including a field having an error correction code;

setting the error correction code for each of the packets; and

injecting errors into one or more of the plurality of packets, such that the corresponding error correction codes are unable to correct these errors.

15. (Original) The method of claim 14, wherein the error correction code is a block code.

16. (Original) The method of claim 14, wherein step (a) further comprises randomly selecting a value and a location for each of the injected errors.

17. (Previously Presented) The method of claim 14, wherein step (c) comprises transmitting the value and the location for each of the injected errors across the second short-range radio communications link.

18. (Previously Presented) The method of claim 1:

wherein step (a) comprises encrypting the data stream with an encryption key; and

wherein step (c) comprises transmitting the encryption key across the second short-range radio communications link.

19. (Previously Presented) The method of claim 1:

wherein step (a) comprises encrypting the data stream with an encryption key; and

wherein step (c) comprises transmitting a decryption key across the second short-range radio communications link, the decryption key corresponding to the encryption key.

20. (Previously Presented) The method of claim 1, wherein the first short-range radio communications link is an ultra wideband (USB) link.

21. (Previously Presented) The method of claim 1, wherein the second short-range radio communications link is a Bluetooth link.

22. (Previously Presented) A wireless communications device, comprising:

means for generating a protected content stream from a data stream;

means for transmitting the protected content stream across a first short-range radio communications link; and

means for transmitting across a second short-range radio communications link information for converting the protected content stream into the data stream;

wherein the protected content stream comprises a packet having one or more inserted errors, the one or more errors at one or more corresponding positions within the packet.

23. (Previously Presented) A method of providing communications security, the method comprising:

(a) receiving a protected content stream from a first short-range radio communications link;

(b) receiving from a second short-range radio communications link information for converting the protected content stream into a data stream; and

(c) generating the data stream from the protected content stream;

wherein the protected content stream comprises a packet having one or more inserted errors, the one or more errors at one or more corresponding positions within the packet.

24. (Canceled)

25. (Previously Presented) The method of claim 23, wherein step (b) comprises receiving the one or more positions and a code for removing the inserted errors from the packet.

26. (Original) The method of claim 25, wherein the code is based on a polynomial.

27. (Original) The method of claim 23, wherein the protected content stream comprises a plurality of data packets and at least one additional packet.

28. (Original) The method of claim 27, wherein step (b) comprises receiving a position of the at least one additional packet in the protected content stream.

29. (Original) The method of claim 28, wherein step (c) comprises removing the at least one additional packet from the protected content stream.

30. (Original) The method of claim 23, wherein the protected content stream in encrypted, and wherein step (b) comprises receiving a key for decrypting the protected content stream.

31. (Previously Presented) The method of claim 23, wherein the first short-range radio communications link is an ultra wideband (USB) link.

32. (Previously Presented) The method of claim 23, wherein the second short-range radio communications link is a Bluetooth link.

33. (Previously Presented) A wireless communications device, comprising:

means for receiving a protected content stream from a first short-range radio communications link;

means for receiving from a second short-range radio communications link information for converting the protected content stream into a data stream; and

means for generating the data stream from the protected content stream;

wherein the protected content stream comprises a packet having one or more inserted errors, the one or more errors at one or more corresponding positions within the packet.

34. (Currently Amended) A wireless communications device, comprising:

a controller configured to generate a protected content stream comprising a packet from a data stream by inserting one or more errors into the packet;

a first transceiver ~~adapted~~ configured to transmit the protected content stream across a first short-range radio communications link; and

a second transceiver ~~adapted~~ configured to transmit across second short-range radio communications link information for converting the protected content stream into the data stream.

35. (Previously Presented) The wireless communications device of claim 34, wherein the first short-range radio communications link is an ultra wideband (UWB) link and the second short-range radio communications link is a Bluetooth link.

36. (Currently Amended) A wireless communications device, comprising:

a first transceiver configured to receive a protected content stream from a first short-range radio communications link, the protected content stream comprising a packet having one or more inserted errors;

a second transceiver configured to receive from a second short-range radio communications link information for converting the protected content stream into a data stream; and

a controller ~~adapted~~ configured to generate the data stream from the protected content stream.

37. (Previously Presented) The wireless communications device of claim 36, wherein the first short-range radio communications link is an ultra wideband (UWB) link and the second short-range radio communications link is a Bluetooth link.

38. (Currently Amended) A computer program stored on a computer useable medium having computer program logic recorded thereon ~~for enabling a processor.~~ ,executable in a computer system, the computer program logic comprising:

program code for enabling ~~the~~ a processor to generate a protected content stream from a data stream, the protected content stream comprising a packet, and the generation of the protected content stream comprising inserting one or more errors into the packet;

program code for enabling the processor to transmit the protected content stream across a first short-range radio communications link; and

program code for enabling the processor to transmit across a second short-range radio communications link information for converting the protected content stream into the data stream.

39. (Currently Amended) A computer program product stored on a computer useable medium having computer program logic recorded thereon ~~for enabling a processor~~ ,executable in a computer system, the computer program logic comprising:

program code for enabling ~~the~~ a processor to receive a protected content stream from a first short-range radio communications link, the protected content stream comprising a packet having one or more inserted errors;

program code for enabling the processor to receive from a second short-range radio communications link information for converting the protected content stream into a data stream; and

program code for enabling the processor to generate the data stream from the protected content stream.

40. (Previously Presented) A method of providing communications security, the method comprising:

(a) generating a protected content stream from a data stream;

(b) transmitting the protected content stream across a first short-range radio communications link; and

(c) transmitting across a second short-range radio communications link information for converting the protected content stream into the data stream;

wherein the protected content stream comprises one or more packets, and wherein step (a) comprises inserting one or more errors in any one or more of the one or more packets.

41. (Previously Presented) The method of claim 40, wherein step (a) further comprises inserting the one or more errors into a portion of any of the one or more packets, the portion at a predetermined position within said packets.

42-43. (Canceled)